WEST Search History

Hide Items | Restore | Clear | Cancel

DATE: Friday, March 19, 2004

Hide?	Set Name	Query	Hit Count
		DB=PGPB,USPT,USOC,EPAB,JPAB,DWPI,TDBD; PLUR=YES; OP=ADJ	
☐	L18	L17 and l9	5
☐	L17	(modify or modifying or modification or encode or encoding)near8 (resource or name)	7682
☐	L16	(calibrating or calibration or calibrate) adj3 domain adj3 (name or address)	2
☐	L15	l9 and l11	0
☐	L14	L13 and l9	0
☐	L13	L12 NOT l7	10
☐	L12	calibrating adj3 (name or address)	12
☐	L11	(encode or encoding) near8 (client or network) near8 address	192
☐	L10	encode near8 (client or network) near8 address	91
☐	L9	20011115	30
☐	L8	(associate or associating) near8 (client or user or host) near8 (DNS or (domain adj3 name adj3 server))	44
☐	L7	calibrating adj3 domain adj3 (name or address)	2
☐	L6	(host or server) near8 (vendor near4 (offering or offer)) same (visitor or machine)	0
☐	L5	(machine-to-machine near8 (communication or exchange))	90
☐	L4	(machine-to-machine near8 (communication or exchange)) same schema	1
☐	L3	machine-to-machine near8 (communication or exchange) near8 schema	0
☐	L2	machine-to-machine near8 (communication or exchange)	90
☐	L1	(host or server) near8 (vendor near4 (offering or offer)) same (visitor or machine) same (data near5 exchange)	0

END OF SEARCH HISTORY

First Hit

Generate Collection

L7: Entry 2 of 2 File: DWPI May 15, 2003

DERWENT-ACC-NO: 2003-576849
DERWENT-WEEK: 200354

TITLE: Client/server associating method using packet-switched network, involves associating identified client according to calibrating domain name, after which client is associated with domain name system server

Basic Abstract Text (1):
NOVELTY - The method involves receiving domain name system (DNS) query from a client DNS server (120), for requesting resolution of a calibrating domain name. A client (110) is identified, based on the calibrating domain name, and the client is associated with the DNS server.

First Hit Fwd Refs

Generate Collection

L18: Entry 2 of 5 File: USPT Oct 15, 2002

DOCUMENT-IDENTIFIER: US 6466570 B1
TITLE: Method of accessing service resource items that are for use in a telecommunications system

Application Filing Date (1):
19980605

Brief Summary Text (39):
The Domain Name System--The DNS is a global, distributed, database, and without its performance, resilience and scalability much of the Internet would not exist in its current form. The DNS, in response to a client request, serves to associate an Internet host domain name with one or more Registration Records (RR) of differing types, the most common being an address (A) record (such as 15.144.8.69) and mail exchanger (MX) records (used to identify a domain host configured to accept electronic mail for a domain). The RRs are distributed across DNS name servers world-wide, these servers cooperating to provide the domain name translation service; no single DNS server contains more than a small part of the global database, but each server knows how to locate DNS servers which are "closer" to the data than it is. For present purposes, the main characteristics of the DNS of interest are: The host name space is organised as a tree-structured hierarchy of nodes with each host having a corresponding leaf node; each node has a label (except the root node) and each label begins with an alphabetic character and is followed by a sequence of alphabetic characters or digits. The full, or "fully qualified" name of a host is the string of node labels, each separated by a ".", from the corresponding leaf node to the root node of the hierarchy, this latter being represented by a terminating "." in the name. Thus a host machine "fred" of Hewlett-Packard Laboratories in Bristol, England will have a fully qualified domain name of "fred.hpl.hp.com." (note that if a host name does not have a terminal "." it is interpreted relative to the current node of the naming hierarchy). Each host has one or more associated Registration Records (RRs). There are a plurality of DNS servers each with responsibility for a subtree of the name space. A DNS server will hold RRs for all or part of its subtree--in the latter case it delegates responsibility for the remainder of the subtree to one or more further DNS servers. A DNS server knows the address of any server to which it has delegated responsibility and also the address of the server which has given it the responsibility for the subtree it manages. The DNS servers thus point to each other in a structuring reflecting that of the naming hierarchy. An application wishing to make use of the DNS does so through an associated "resolver" that knows the address of at least one DNS server. When a DNS server is asked by this resolver for an RR of a specified host, it will return either the requested RR or the address of a DNS server closer to the server holding the RR in terms of traversal of the naming hierarchy. In effect, the hierarchy of the servers is ascended until a server is reached that also has responsibility for the domain name to be resolved; thereafter, the DNS server hierarchy is descended down to the server holding the RR for the domain name to be resolved. The DNS uses a predetermined message format (in fact, it is the same for query and response) and uses the IP protocols.

Detailed Description Text (75):
As regards updating service resources, there is likely to be a need to update certain data items on a fairly frequent basis (for example, roaming number). Where

the PSTN operator does not place any controls on the service resources 49, then update is a relatively simple matter, only requiring write access to the server concerned (as already indicated, this will generally involve one or more levels of password protection). However, where the PSTN operator exercises control over the service resources, for example by only permitting customisations of standard service resources, such customised resources being loaded on servers controlled by the operator), then write access to the service resource may be tightly controlled. Again, an HTML form may conveniently be used as the medium for modifying a data item in such cases; to the operator, this has the benefit of limiting the modifications possible whilst to the user, a form interface should provide a simple route to resource modification.

Generate Collection

L18: Entry 3 of 5 File: USPT Aug 28, 2001

DOCUMENT-IDENTIFIER: US 6282281 B1
** See image for Certificate of Correction **
TITLE: Method of providing telecommunications services

Application Filing Date (1):
19980603

Brief Summary Text (39):
The Domain Name System--The DNS is a global, distributed, database, and without its performance, resilience and scalability much of the Internet would not exist in its current form. The DNS, in response to a client request, serves to associate an Internet host domain name with one or more Registration Records (RR) of differing types, the most common being an address (A) record (such as 15.144.8.69) and mail exchanger (MX) records (used to identify a domain host configured to accept electronic mail for a domain). The RRs are distributed across DNS name servers world-wide, these servers cooperating to provide the domain name translation service; no single DNS server contains more than a small part of the global database, but each server knows how to locate DNS servers which are "closer" to the data than it is. For present purposes, the main characteristics of the DNS of interest are:

Detailed Description Text (83):
As regards updating service resources, there is likely to be a need to update certain data items on a fairly frequent basis (for example, roaming number). Where the PSTN operator does not place any controls on the service resources 49, then update is a relatively simple matter, only requiring write access to the server concerned (as already indicated, this will generally involve one or more levels of password protection). However, where the PSTN operator exercises control over the service resources, for example by only permitting customisations of standard service resources, such customised resources being loaded on servers controlled by the operator), then write access to the service resource may be tightly controlled. Again, an HTML form may conveniently be used as the medium for modifying a data item in such cases; to the operator, this has the benefit of limiting the modifications possible whilst to the user, a form interface should provide a simple route to resource modification.

DOCUMENT-IDENTIFIER: US 6246758 B1
TITLE: Method of providing telecommunication services

Application Filing Date (1):
19980604

Brief Summary Text (47):
The Domain Name System--The DNS is a global, distributed, database, and without its performance, resilience and scalability much of the Internet would not exist in its current form. The DNS, in response to a client request, serves to associate an Internet host domain name with one or more Registration Records (RR) of differing types, the most common being an address (A) record (such as 15.144.8.69) and mail exchanger (MX) records (used to identify a domain host configured to accept electronic mail for a domain). The RRs are distributed across DNS name servers world-wide, these servers cooperating to provide the domain name translation service; no single DNS server contains more than a small part of the global database, but each server knows how to locate DNS servers which are "closer" to the data than it is. For present purposes, the main characteristics of the DNS of interest are:

Detailed Description Text (85):
As regards updating service resources, there is likely to be a need to update certain data items on a fairly frequent basis (for example, roaming number). Where the PSTN operator does not place any controls on the service resources 49, then update is a relatively simple matter, only requiring write access to the server concerned (as already indicated, this will generally involve one or more levels of password protection). However, where the PSTN operator exercises control over the service resources, for example by only permitting customisations of standard service resources, such customised resources being loaded on servers controlled by the operator), then write access to the service resource may be tightly controlled. Again, an HTML form may conveniently be used as the medium for modifying a data item in such cases; to the operator, this has the benefit of limiting the modifications possible whilst to the user, a form interface should provide a simple route to resource modification.

First Hit Fwd Refs

Generate Collection

L18: Entry 5 of 5 File: USPT Oct 10, 2000

DOCUMENT-IDENTIFIER: US 6131095 A
** See image for Certificate of Correction **
TITLE: Method of accessing a target entity over a communications network

Application Filing Date (1):
19980609

Brief Summary Text (30):
The Domain Name System--The DNS is a global, distributed, database, and without its performance, resilience and scalability much of the Internet would not exist in its current form. The DNS, in response to a client request, serves to associate an Internet host domain name with one or more Registration Records (RR) of differing types, the most common being an address (A) record (such as 15.144.8.69) and mail exchanger (MX) records (used to identify a domain host configured to accept electronic mail for a domain). The RRs are distributed across DNS name servers world-wide, these servers cooperating to provide the domain name translation service; no single DNS server contains more than a small part of the global database, but each server knows how to locate DNS servers which are "closer" to the data than it is. For present purposes, the main characteristics of the DNS of interest are:

Detailed Description Text (87):
As regards updating service resources, there is likely to be a need to update certain data items on a fairly frequent basis (for example, roaming number). Where the PSTN operator does not place any controls on the service resources 49, then update is a relatively simple matter, only requiring write access to the server concerned (as already indicated, this will generally involve one or more levels of password protection). However, where the PSTN operator exercises control over the service resources, for example by only permitting customisations of standard service resources, such customised resources being loaded on servers controlled by the operator), then write access to the service resource may be tightly controlled. Again, an HTML form may conveniently be used as the medium for modifying a data item in such cases; to the operator, this has the benefit of limiting the modifications possible whilst to the user, a form interface should provide a simple route to resource modification.

First Hit

Generate Collection

L28: Entry 1 of 7 File: PGPB Feb 27, 2003

DOCUMENT-IDENTIFIER: US 20030039240 A1
TITLE: Methods, systems and computer program products for accessing an embedded web server on a broadband access terminal

Application Filing Date:
20010824

Detail Description Paragraph:
[0023] As is further illustrated in FIG. 1, the service provider network 38 may include a dynamic host configuration protocol (DHCP) server 32 which assigns Internet Protocol (IP) addresses to devices, such as the broadband access terminals 12, 12' and the customer premises equipment 20, 20', 20". A domain name server (DNS) 34 may also be provide so as to resolve domain names to an IP address. Additionally, a gateway 36 may provide access from the service provider network 38 to the Internet 40 or other such networks, so as to allow access to a web server 42 which is outside the service provider network 38.

CLAIMS:

16. The broadband access terminal of claim 15, wherein the monitor circuit is further configured to identify a dynamic host configuration protocol (DHCP) packet destined for the user terminal, extract an Internet Protocol (IP) address of the user terminal, a Media Access Control (MAC) address of the user terminal and an IP address of the at least one of the domain name server and the network gateway from the identified DHCP packet, determine a MAC address of the at least one of the domain name server and the network gateway based on the IP address of the at least one of the domain name server and the network gateway and associate the IP address of the user terminal, the MAC address of the user terminal, the IP address of the at least one of the domain name server and the network gateway and the MAC address of the at least one of the domain name server and the network gateway .

21. The broadband access terminal of claim 19, wherein the ARP proxy circuit is further configured to determine if a valid MAC address of the at least one of the domain name server and the network gateway is associated with the user terminal; and wherein the ARP proxy circuit is configured to send an ARP response containing a MAC address of the at least one of the domain name server and the network gateway associated with the user terminal to the user terminal if the ARP request is from the user terminal and a valid MAC address of the at least one of the domain name server and the network gateway is associated with the user terminal; and wherein the ARP proxy circuit is configured to send an ARP response to the user terminal, the ARP response containing a MAC address of the broadband access terminal, if a valid MAC address of the at least one of the domain name server and the network gateway is not associate with the user terminal.

First Hit

Generate Collection

L28: Entry 2 of 7 File: PGPB Aug 29, 2002

DOCUMENT-IDENTIFIER: US 20020120607 A1
TITLE: File sharing system for serving content from a computer

Application Filing Date:
20010801

Summary of Invention Paragraph:
[0009] The guest module resolves a domain name to a current IP address of a subscriber computer, and monitors the subscriber computers to determine which of the subscriber computers are online, and if online, redirects a computer originating the browser request to the appropriate subscriber computer. The guest module also handles subsequent requests, such as hyperlink selections, originating from the web browser application and redirects such requests to the appropriate subscriber computer.

Detail Description Paragraph:
[0036] The server 16 preferably functions as a ubiquitous touch point, servicing requests from subscribers, partners, and guests using the system. The server 16 is preferably composed of different modules, which are shown in FIG. 2. In FIG. 2, the server 16 is shown comprised of four distinct modules, including a subscriber module 30, a guest module 32, a management API module 18, and daemons 34 for managing e-mail and verifying subscribers' DNS Internet connectivity, i.e., ensuring that a subscriber's domain name resolves to the server 16. The subscriber module 30 is responsible for communications with the Active Node 10. It responds to a variety of message requests as they are received from the Active Node 10 by confirming or rejecting such requests.

Detail Description Paragraph:
[0037] The guest module 32 deals with requests that originate from a guest's web browser. This includes lookups to resolve a domain name to a subscriber's current IP address. The guest module 32 also sends a message to the subscriber's machine to determine whether it is currently online and, if so, redirects the request to connect the guest directly to the subscriber's machine. If the subscriber is not currently online, the guest module 32 may render an appropriate response page to so indicate.

Detail Description Paragraph:
[0043] FIG. 4A illustrates operation of the inbound API 40 utilizing the "AddSite" function. As shown in FIG. 4A, an end-user may visit a partner's web site in search of a domain name and a hosting option, for example by accessing a website associated with the partner via the Internet (Step 50). The end-user may elect the service described herein and proceed to the registration process. Once the information is successfully gathered, the partner may transmit the end-user's information to the server 16, for example by invoking the "AddSite" function from the inbound API 40 (Step 51) which causes a particular message to be transmitted to the server 16 in order to create an end-user account by writing a record to its database. The server 16 may respond with an acknowledgement message, or alternatively, an error message if there is an error in receiving the information (Step 52). If an error is encountered, the "AddSite" function may again be invoked and a message may again be transmitted to the server 16 (FIG. 1) as described above

(Step 53a). Otherwise, the partner may associate the IP address for the end-user's domain name to the server 16 (Step 53b), and the end-user may be presented with a confirmation web page (and/or an e-mail message) indicating to the end-user how to proceed with installation and configuration of the service (Step 54).

Detail Description Paragraph:
[0051] Returning to FIG. 1, the client application 10 allows subscribers to transform their own computer into a uniquely identifiable server, capable of publishing content over the public Internet. It communicates with the server 16 allowing discovery and resolution of domain names to a dynamically changing IP address. It also permits the subscriber to activate and configure the system as well as manage and publish the content. Activation allows the system to resolve domain names to dynamically changing IP addresses. For example, whenever the machine's IP address changes, this triggers an event which transmits and persists the new information in the database. This information is subsequently used by the guest module 32 (FIG. 2) which provides the lookup and redirect from a domain name to the appropriate IP address.

Detail Description Paragraph:
[0068] A standard web browser (i.e., Internet Explorer, Netscape, etc.) is used to view the website of a subscriber. When a guest enters the URL of a subscriber's website into a browser, the request is handled by the server 16. Initial requests may occur over a non-secure connection. The guest module 32 (FIG. 2) in the server 16 resolves the mapping from the domain name to the subscriber's current IP address. If the subscriber's machine is currently online, the guest module 32 will redirect the request to the subscriber's computer. The redirect to the subscriber's website will also occur over a non-secure channel unless the subscriber has configured a private site, in which case the login transaction will occur over HTTP/S. If the subscriber's machine is found to be offline, the server 16 may display an "away page" notifying the guest to try again later.

CLAIMS:

11. The system of claim 10, wherein the guest module resolves a domain name to a current IP address of a subscriber computer, and monitors the subscriber computers to determine which of the subscriber computers are online, and if online, redirects a computer originating the request to the appropriate subscriber computer.

First Hit Fwd Refs

Generate Collection

L28: Entry 3 of 7 File: USPT Feb 3, 2004

DOCUMENT-IDENTIFIER: US 6687746 B1
TITLE: System apparatus and method for hosting and assigning domain names on a wide area network

Application Filing Date (1):
19990830

Detailed Description Text (25):
When any network user, including a client, enters a request into the browser for an assigned domain name, such as, for example, http://sitenamei.webjump.com, the DNS resolves the requested domain name to its Virtual Internet Protocol ("VIP") address. By default, incoming browser requests for any subdomain to "providerdomainname.com" is forwarded to the host VIP address for the domain "providerdomainname.com". This is achieved by including the wildcard entry into the domain's zone file in the form of "*.providerdomainname.com" as shown in FIG. 4 for webjump.com. Thus, instead of the zone file including all possible subdomain names, such as, "sitename.providerdomainname.com", wherein each subdomain would have its own IP address, the request is directed to the address of the wildcard entry "*.providerdomainname.com". For example, in one embodiment, the domain name "sitename.webjump.com" resolves to 216.49.10.200, wherein "webjump.com" is the provider chosen domain name. The resolved VIP address is then transmitted to the domain retrieval system.

CLAIMS:

1. A method for enabling internet access to content located by a domain name, the domain name including a user-selected subdomain label that is not associated with an IP address in a zone file of any higher-level domain, the method comprising: operating a host having an IP address specified by an internet-class resource record for a domain name server, in that the resource record associates the host IP address to a host domain name in a zone file of the domain name server, and wherein the host domain name comprises (a) a subdomain labeled with a designated wildcard character of a domain name system and (b) at least one: higher-level domain name; configuring a content address according to a content storage system of the host independently of the domain name system, the content address comprising a user-selected label, wherein the user-selected label comprises at least one character that is not the designated wildcard character; storing content in the content storage system, the content addressed by the content address; receiving a domain name configured in accordance with the domain name system, the domain name comprising the host domain name with the user-selected label substituted for the designated wildcard character; determining the content address from the user-selected label; retrieving the content from the content storage system using the content address; and serving the content.

12. A system for enabling internet access to content identified by a user-selected domain name comprising a subdomain, without requiring that the subdomain be associated with an IP address of a higher-level domain, the system comprising: an internet-connected host computer, the host computer having an IP address specified by an internet-class resource record for a domain name server, wherein the resource record associates the host IP address to a host domain name in a zone file of the

domain name server, and wherein the host domain name comprises (a) a subdomain labeled with a designated wildcard character of a domain name system and (b) at least one higher-level domain name; a memory operably associated with the host computer, the memory holding instructions comprising: configuring a content address according to a content storage system of the host computer independently of the domain name system, the content address comprising a user-selected label, wherein the user-selected label comprises at least one character that is not the designated wildcard character; storing content in the content storage system, the content addressed by the content address; receiving a domain name configured in accordance with the domain name system, the domain name comprising the host domain name with the user-selected label substituted for the designated wildcard character; determining the content address from the user-selected label; retrieving the content from the content storage system using the content address; and serving the content.

First Hit Fwd Refs

Generate Collection

L28: Entry 4 of 7 File: USPT Oct 15, 2002

DOCUMENT-IDENTIFIER: US 6466570 B1
TITLE: Method of accessing service resource items that are for use in a telecommunications system

Application Filing Date (1):
19980605

Brief Summary Text (39):
The Domain Name System--The DNS is a global, distributed, database, and without its performance, resilience and scalability much of the Internet would not exist in its current form. The DNS, in response to a client request, serves to associate an Internet host domain name with one or more Registration Records (RR) of differing types, the most common being an address (A) record (such as 15.144.8.69) and mail exchanger (MX) records (used to identify a domain host configured to accept electronic mail for a domain). The RRs are distributed across DNS name servers world-wide, these servers cooperating to provide the domain name translation service; no single DNS server contains more than a small part of the global database, but each server knows how to locate DNS servers which are "closer" to the data than it is. For present purposes, the main characteristics of the DNS of interest are: The host name space is organised as a tree-structured hierarchy of nodes with each host having a corresponding leaf node; each node has a label (except the root node) and each label begins with an alphabetic character and is followed by a sequence of alphabetic characters or digits. The full, or "fully qualified" name of a host is the string of node labels, each separated by a ".", from the corresponding leaf node to the root node of the hierarchy, this latter being represented by a terminating "." in the name. Thus a host machine "fred" of Hewlett-Packard Laboratories in Bristol, England will have a fully qualified domain name of "fred.hpl.hp.com." (note that if a host name does not have a terminal "." it is interpreted relative to the current node of the naming hierarchy). Each host has one or more associated Registration Records (RRs). There are a plurality of DNS servers each with responsibility for a subtree of the name space. A DNS server will hold RRs for all or part of its subtree--in the latter case it delegates responsibility for the remainder of the subtree to one or more further DNS servers. A DNS server knows the address of any server to which it has delegated responsibility and also the address of the server which has given it the responsibility for the subtree it manages. The DNS servers thus point to each other in a structuring reflecting that of the naming hierarchy. An application wishing to make use of the DNS does so through an associated "resolver" that knows the address of at least one DNS server. When a DNS server is asked by this resolver for an RR of a specified host, it will return either the requested RR or the address of a DNS server closer to the server holding the RR in terms of traversal of the naming hierarchy. In effect, the hierarchy of the servers is ascended until a server is reached that also has responsibility for the domain name to be resolved; thereafter, the DNS server hierarchy is descended down to the server holding the RR for the domain name to be resolved. The DNS uses a predetermined message format (in fact, it is the same for query and response) and uses the IP protocols.

Brief Summary Text (44):
Rather than a resolver being responsible for carrying out the series of query iterations required to resolve a domain name, the resolver may specify its first

query to be recursive in which case the receiving DNS server is responsible for resolving the query (if it cannot directly return the requested RR, it will itself issue a recursive query to a `closer` DNS server, and so on).

Detailed Description Text (24):
An alternative lookup solution is to use a hierarchically-structured distributed database system, similar to (or even part of) the Domain Name System (DNS) of the Internet, in order to resolve the UI part of a resource code to a corresponding URI. This approach, which will be described in more detail below, would typically involve databases maintained by each PSTN operator for its numbers with which URIs are associated. These databases would be accessible by all PSTNs through a network such as the Internet with resolution requests being pointed to the appropriate database in a manner similar to the Domain Name System. In this case, the block 47 is constituted by an appropriate resolution program arranged to request UI resolution over the Internet through interface 44.